Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE
2010

2. REPORT TYPE

3. DATES COVERED
00-00-2010 to 00-00-2010

4. TITLE AND SUBTITLE
Quick Reaction Test: Host-Based Security System

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Joint Interoperability Test Command,3341 Strauss Avenue Suite 236,Indian Head,MD,20640

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:

a. REPORT
unclassified

b. ABSTRACT
unclassified

c. THIS PAGE
unclassified

17. LIMITATION OF ABSTRACT
Same as Report (SAR)

18. NUMBER OF PAGES
2

19a. NAME OF RESPONSIBLE PERSON

ITEA Journal 2010; 31: 447–448

Quick Reaction Test: Host-Based Security System

Timothy K. Holmes
Joint Interoperability Test Command, Indian Head, Maryland
Cesar E. Pie
Cyber Security Research and Solutions Corporation, La Plata, Maryland

Under the leadership and shared vision of the United States Strategic Command, the Defense Information Systems Agency (DISA) Mission Assurance/Network Operations Program Executive Office, the DISA Joint Interoperability Test Command, and other Department stakeholders, the Department of Defense has successfully orchestrated a Global Information Grid–wide initiative in support of the institutionalization of the Host-Based Security System throughout the Department of Defense. The scope of the Host-Based Security System deployment will be worldwide. This vast effort requires a large support infrastructure to be in place and a rigorous testing project that will help expedite the fielding of its unique capabilities.

Key words: Computer network defense; computer system security; cyber-threat; intrusion detection; intrusion prevention.

The Host-Based Security System (HBSS) baseline is a flexible, Commercial-Off-The-Shelf (COTS)-based application. It monitors, detects, and counters known cyber-threats to the Department of Defense (DoD) Enterprise. Under the sponsorship of the Enterprise-wide Information Assurance and computer Network Defense Solutions Steering Group (ESSG), the HBSS solution will be attached to each host (i.e., server, desktop, and laptop) in DoD. The system will be managed by local administrators and configured to address known exploit traffic using an intrusion prevention system (IPS) and host firewall. The Defense Information Systems Agency (DISA) Program Executive Office Mission Assurance and Network Operations (PEO-MA) is providing the program management and supporting the deployment of this solution.

Joint test approach

Under the auspices of the Joint Test and Evaluation Program, the HBSS Quick Reaction Test (QRT) project is focused to develop tactics, techniques, and procedures (TTP) and concepts of operations (CONOPS) in support of HBSS operations. The QRT has taken a joint approach (as well as assessment practices, principles, and strategies used in previous Bulwark Defender exercises) to test formal and informal HBSS configuration policies across the Global Information Grid (GIG) and to develop DoD-specific protection level baselines to address the required level of security needed by the Department. These configuration baselines will provide GIG network defenders with documented TTP and CONOPS for the employment, implementation, and operation of the HBSS throughout DoD (enhancing the warfighter's ability and capabilities to protect, monitor, detect, analyze, diagnose, and respond to cyber threats). The United States Strategic Command (USSTRATCOM) through United States Cyber Command (USCYBERCOM) has instructed the potential use of the QRT test results in upcoming Operational Plans (OPLANS) and will require implementation of HBSS TTP recommendations by their DoD Network Operations (NetOps) Combatant Commands/Services/Agencies (CC/S/A) via Fragmentary Orders (FRAGO) and/or Command Task Orders (CTO).

The HBSS QRT test approach is based on the proven Joint Interoperability Test Command (JITC) Information Assurance/Computer Network Defense (IA/CND) attack-based methodology. Much like a typical war game exercise, the JITC approach uses a red attack/blue defend construct. The concept is red attacking along defined attack vectors, aligned with an anatomy of an attack with detailed scenarios based on the latest Joint Task Force-Global Network Operations (JTF-GNO) J2 observed threats. Blue will use the full range of people, processes, and technologies available to defend against red. Each attack and defend activity is controlled, measured, and correlated, with analysis focusing on the most effective and suitable scenario as it relates to the warfighter's mission. The operational threat environment replicated by the threat team will aim to target second and third generation threats, as defined in the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E. This is the replication of non-state–sponsored groups utilizing common tools in a sophisticated manner and the replication of state-sponsored groups utilizing a combination of common and uncommon hacker tools and techniques in a sophisticated manner with unlimited resources.

As prioritized by USSTRATCOM, every recommended scenario event has been mapped to its corresponding class of attack (i.e., passive, active, insider, distribution, and close-in) and three of seven stages of an anatomy of attack (i.e., gaining access, escalation of privilege, maintaining access). To support the development of attack scenarios, the JITC created the HBSS QRT Threat Team Working Group (TTWG) to identify, coordinate, and validate the selected scenarios. The scenarios were created by the U.S. Air Force and DISA Field Security Officer and reviewed by the National Security Agency. The JITC, in coordination with the TTWG, will continue to add increasingly sophisticated scenarios over the life of the QRT to render the best possible HBSS configurations and TTP.

Test concept and measures

As part of each QRT event, the threat team will render a series of increasingly sophisticated attacks. The blue defenders will implement a series of candidate configurations of TTP in an attempt to counter the threat. The test concept will measure the relative performance of these candidate configurations and TTPs to identify the best candidate. The measures the QRT will use are taken from the Office of the Secretary of Defense (OSD) Director, Operational Test and Evaluation Core Metrics Manual for Operational Assessments of Information Assurance and Interoperability (DOT&E Core Metrics Manual). This manual contains the performance-based metrics used in the DOT&E-sponsored assessments of IA/CND during Combatant Command (COCOM) exercises. The DOT&E Core Metrics Manual defines the performance measures and metrics, the data elements, and the analysis method, along with associated data collection forms. This Manual has been applied to a variety of COCOM exercises, including Bulwark Defender, to measure the operational performance of the COCOM's IA/CND capability. The metrics are proven, accepted by all OTAs, well understood, and will yield the exact performance-based criteria needed by the HBSS QRT to determine the most effective configurations and TTPs.

Conclusion

The HBSS QRT will be accomplished in two spirals; each spiral will consist of a set of two lab-based events and conclude with an operational test that includes the participation of both U.S. Pacific Command and U.S. Strategic Command. The HBSS QRT was directed on January 6, 2010, with an expected performance period ending January 5, 2011. Upcoming HBSS QRT events will allow the warfighter to establish best practices and obtain lessons learned. The HBSS QRT will provide results that will undoubtedly expand the warfighter's capability to protect, detect, diagnose, and react to cyber threats using effective configurations and improved TTPs. ❑

MR. KEVIN HOLMES serves as the JITC information assurance technical advisor, where he develops and maintains the Command's IA policies, methodologies and capabilities. Mr. Holmes joined the JITC shortly after its inception in 1989. He has held a variety of positions within the Command. Mr. Holmes started his JITC career developing software for many JITC instrumentation systems ranging from tactical message protocol analyzers to modeling and simulating Tactical Data Systems. He stood up the JITC IA capability in 2001 and has been working in that area since. Holmes earned his bachelor of science degree in management information systems (MIS) from the University of Arizona and his master of science degree in computer science from George Mason University. E-mail: kevin.holmes@disa.mil

MR. CESAR E. PIE is chief executive officer of Cyber Security Research and Solutions Corporation (CSRS-Corp). He has extensive program management expertise and has provided subject matter expert support to the JITC for over 6 years in the fields of information system security engineering, information assurance, and computer network operations (computer network attack, computer network exploitation, and computer network defense). Mr. Pie graduated from the University of Maryland University College with a master of science degree from the Computer System Management—Information Assurance Program that is supported by the Department of Homeland Security and the National Security Agency's Center of Academic Excellence in Information Assurance Education (CAE/IAE). Among others, a few of Mr. Pie's certification credentials include Certified in the Governance of Enterprise Information Technology (CGEIT), Information System Security Engineering Professional (ISSEP), Certified Information Systems Auditor (CISA), Certified Information System Security Professional (CISSP), and Project Management Professional (PMP). E-mail: cesar.pie@csrscorp.com

References

DoD. 2008. Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.01E. *Information Assurance and Computer Network Defense.* Washington, DC: DoD.